FY2024

CCHMIS ADMINISTRATION MANUAL

Policies and Procedures of the CARES of NY, Inc. Collaborative Homeless Management Information System (CCHMIS).

VERSION 1.4
EFFECTIVE: FEBRUARY 1, 2024

CARES OF NY, INC
ENDING HOMELESSNESS

Contents

Version History

REVISION NUMBER	REVISION DATE	REVISION BY	DESCRIPTION OF CHANGE
1.0	10/01/2019	Allyson Thiessen and Emily Rebehn	Reformatting and Update
1.1	7/01/2020	Allyson Thiessen	Update and Project name change
1.2	10/01/2020	Allyson Thiessen	Update
1.3	10/01/2022	Kelli Clark	Update
1.4	12/01/2023	Kelli Clark and Megan Clark	Formatting and Updates to reflect HUD FY2024 HMIS Data Standards

Introduction

CARES of NY, Inc. (CARES) has developed the following Administration Manual (hereafter referred to as "this document") to serve as a reference regarding the administration of the CARES Collaborative Homeless Management Information System.

This document defines the goals and objectives of the CARES Collaborative HMIS (CCHMIS) program, provides the roles and responsibilities of those involved in the program, and establishes policies for the operation of the CCHMIS. This includes CCHMIS administration, communication, security, privacy, and data quality.

Background

The CARES Collaborative HMIS

CARES of NY, Inc. (CARES) is a not-for-profit organization with a mission to collaborate with and support local communities towards the creation of systems to end, and prevent future, homelessness. CARES is the HMIS Lead for the CARES Collaborative HMIS (CCHMIS), a multi-Continuum HMIS that serves communities across central and upstate New York State. The CoC's included in this HMIS are:

NY – 503 ACCH	NY – 507 HSPB	NY 512- RCHSC
NY – 519 CGHC	NY – 520 FEHC	NY – 522 PNHC
NY – 523 SNC	NY – 525 NY BOS	NY – 601 DCCoC
NY – 602 OCHC	NY – 606 RCCC	NY – 608 UCCC

To fulfill the requirements of the Continuum of Care Program (CFR Title 24 Part 578) as updated and published April 1, 2017, CARES uses the Affordable Wider Area Regional Database System (AWARDS) software from vendor Foothold Technology. Foothold Technology, as the HMIS Vendor, maintains the database in compliance with HUD specifications to preserve the integrity, security, and privacy of the data within the CCHMIS.

History of HMIS

In 2001, the United States Congress directed the U.S. Department of Housing and Urban Development (HUD) to provide an annual report on the status of homelessness across the country[1]. To meet this demand, HUD put forth the Homeless Management Information Systems (HMIS): Data and Technical Standards Final Notice, effective August 30, 2004, for a computerized data collection system or Homeless Management Information System (HMIS) that records the characteristics, demographic information, and number of persons using homeless services across location and over time.

As per this Notice, "the development of a local HMIS is about:

(1) Bringing the power of computer technology to the day-to-day operations of individual homeless assistance providers;

(2) knitting together providers within a local community in a more coordinated and effective housing and service delivery system for the benefit of homeless clients; and

(3) obtaining and reporting critical aggregate information about the characteristics and needs of homeless persons. An HMIS provides significant opportunities to improve access to, and delivery of, housing and services for people experiencing homelessness. An HMIS can accurately describe the scope of homelessness and the effectiveness of efforts to ameliorate it. An HMIS can strengthen community planning and resource allocation."

HUD put forth further guidance in The HMIS Proposed Rule of 2011 (24 CFR Parts 91, 576, 580, and 583- the Homeless Management Information Systems Requirements), and currently maintains the HMIS Data Standards and HMIS Data Dictionary to provide a standard method for recording information in the HMIS.

As a result, the HMIS provides a common language for discussion about the quality and quantity of services, acts a basis for evaluation at the community, state, and federal levels to be used for allocation of funding and the improvement of community planning.

HMIS Governance

As a multi-Continuum HMIS, the CCHMIS will have a single, joint HMIS Governance Charter that applies to the HMIS Lead and all Continuums of Care that choose to participate in the CCHMIS. The HMIS Lead will

[1] Discussed within Homeless Management Information Systems (HMIS): Data and Technical Standards Final Notice, effective August 30, 2004: 1.2.1. Direction to HUD on Homeless Management Information Systems.

develop and maintain, with review and approval by all participating Continuums, this joint CCHMIS Governance Charter.

- At minimum, the CCHMIS Governance Charter must include:
    1. A requirement that the Continuum and the HMIS Lead enter into a formal agreement (Memorandum of Understanding) representative of the HMIS Lead designation that outlines management processes, responsibilities, decision-making structures, and oversight of the HMIS project;
    2. A requirement that the HMIS Lead enter into written HMIS Participation Agreements with each CHO requiring the CHO to comply with all privacy, security, and data quality requirements and imposing sanctions for failure to comply; and
    3. Addresses fees for participation in the HMIS.
- As the CCHMIS is a multi-Continuum HMIS, the CCHMIS Governance Chart must also specify:
    1. That each Continuum of Care designates the same information system as the official HMIS software; and
    2. That all Continuums of Care designate the same HMIS Lead and must work jointly with the HMIS Lead to develop and adopt a joint governance charter;
    3. That all Continuums of Care within a multi-continuum HMIS designate the same governance, technical, security, privacy, and data quality standards; and
    4. That to be a multi-Continuum HMIS, the HMIS must be capable of reporting unduplicated data for each Continuum of Care separately.

Roles and Responsibilities

Continuum of Care

The Continuum of Care is responsible for making decisions about HMIS management and administration and is responsible for ensuring that its HMIS is operated in accordance with all applicable federal, state, and local laws and regulations.

The Continuum must:

- Designate a single information system as the official Homeless Management Information System (HMIS) software for the geographic area, and ensure the software meets all HUD HMIS requirements;
- Designate an eligible applicant (be a state or local government, an instrumentality of state or local government, or a private nonprofit organization) to manage the Continuum's HMIS, which will be known as the HMIS Lead;
- Ensure consistent participation in the HMIS by recipients of funds from the Emergency Solutions Grants Program and from the other programs authorized by Title IV of the McKinney-Vento Act across the geographic area of the Continuum;
- Work with the HMIS Lead to:
    1. Ensure the HMIS is operated in compliance with requirements prescribed by HUD.
        i. Ensure the HMIS software can report unduplicated data for each Continuum of Care to support the multi-Continuum HMIS configuration.

ii. Ensure that HMIS processing capabilities remain consistent with the privacy obligations of the CHO;

2. Develop and maintain an HMIS governance charter;
3. Ensure each CHO enters into a CCHMIS CHO Agreement (participation and confidentiality agreement);
4. Ensure CHOs meet or exceed data quality requirements;
5. Review, revise, and approve the policies and plans developed by the HMIS Lead for the HMIS as necessary or required by HUD and ensure these plans include a privacy plan, a security plan, and a data quality plan;

» Maintain documentation evidencing compliance with the governance charter; and

» Be responsible for ensuring HMIS data is collected to a centralized location at least once a year from all Users within the Continuum;

» Approve any additional data elements for HMIS collection and entry for specific programs within the Continuum or for the Continuum as a whole; and

» Be responsible for imposing sanctions on CHOs for failure to comply with any HMIS requirements, as per applicable federal rules.

HMIS Lead

The HMIS Lead is designated by the Continuum of Care and will be responsible for facilitating the success of the HMIS for all participating organizations within a Continuum, including implementing and administrating the HMIS; conducting oversight of the HMIS; and taking corrective action, if needed, to ensure that the HMIS is compliant with all federal HMIS requirements.

The HMIS Lead must:

» Provide system administration and operation:

1. Sign a contract with an HMIS vendor for HMIS database software and services and ensure that this contract requires the HMIS Vendor to meet HUD and other federal regulations and standards;
2. Handle the billing and payments for the HMIS software;
3. Execute a written CCHMIS CHO Agreement (participation and confidentiality agreement) with each CHO which includes the obligations and authority of the HMIS Lead and CHO, and an agreement that the HMIS Lead and the CHO will process Protected Identifying Information consistent with the agreement;
4. Maintain a level of staffing to fulfill the requirements of the HMIS Lead in all contracts and agreements;
5. Provide HMIS-related services via Technical Assistance contracts;

» Provide HMIS training:

1. Provide ongoing training, technical assistance, database management, and reporting support to the CHOs;
2. Provide Help Desk operation and End User support for the HMIS;

» Engage in governance, management, and collaboration with the Continuum to:

1. Ensure participation by recipients of funds from the Emergency Solutions Grants Program and from the other programs authorized by Title IV of the McKinney-Vento Act;

2. Ensure the HMIS software can report unduplicated data for each Continuum of Care to support the multi-Continuum HMIS configuration.
3. Submit reports to HUD as required;
4. Serve as the applicant to HUD for grant funds to be used for HMIS activities for the Continuum of Care's geographic area, as directed by the Continuum, and, if selected for an award by HUD, enter into a grant agreement with HUD to carry out the HUD-approved activities;

» Engage in policy development and implementation by:
1. Developing written policies and procedures for the operation of the HMIS that apply to the HMIS Lead, its CHOs, and the Continuum of Care, and ensure that these comply with all applicable federal law and regulations, and applicable state or local governmental requirement;
2. Developing and maintaining written plans (Privacy, Security, Data Quality);

» Provide monitoring and oversight for the HMIS by:
1. Developing data quality benchmarks;
2. Monitoring and enforcing compliance of all CHOs with HMIS requirements and report on compliance to the Continuum;

» Engage in data analysis/reporting on the HMIS by:
1. Providing data to CHOs to monitor data quality;
2. Assisting CHOs with data analysis for grant writing; and
3. Providing data to Data Committees, which Data Committees use to make recommendations and providing guidance to their respective Continuums.

Contributing Homeless Organization

A Contributing Homeless Organization (or "CHO") in the Continuum will enter into a contract for HMIS services with the Continuum's chosen HMIS software vendor (through the HMIS Lead or directly through an independent contract with the HMIS vendor) and will enter data into the HMIS as required, including – to the best of their ability – meeting any completeness, quality, and timeliness requirements. A CHO will also be responsible for the compliance of their staff with respect to maintaining the confidentiality of client-level HMIS data and will ensure compliance with all State and Federal regulations, including HIPAA requirements, as they apply to their organization.

A CHO must:

» Enter a contract for HMIS services with the Continuum's chosen HMIS software vendor:
1. Through a contract with the HMIS Lead; or
2. Directly with the HMIS vendor through an independent contract.
    i. These organizations are referred to as Vendor CHOs within this document.

***PLEASE NOTE**: Vendor CHOs will not receive all HMIS services from the HMIS Lead, but **are** required to follow all policies for CHOs as described within this document unless specifically exempted within the policy;*

» Enter into a CCHMIS CHO Agreement with the HMIS Lead that will outline the requirements of the CHO and the HMIS Lead to ensure a successful HMIS implementation, which will include that the CHO will:

1. Be held responsible for any misuse of the HMIS by its Users.
2. Designate a staff member to be the Agency HMIS Administrator for the CHO;
3. Comply with all privacy and security requirements outlined in this document, as well as requirements in the CHO HMIS Agreement;
4. Comply with Federal, state, and local laws that require additional privacy or confidentiality protections; and
5. Implement procedures to monitor and ensure its compliance with applicable agreements and HUD requirements, including enforcement of sanctions for noncompliance, as an organization with access to protected identifying information, including monitoring for and enforcing staff compliance in all activities associated with User access of the HMIS.

Agency HMIS Administrator

The Agency HMIS Administrator will receive additional HMIS training and will be responsible for the data quality, security, and privacy of the CHO's use of the HMIS.

The Agency HMIS Administrator must:

- Ensure the CHO is in compliance with privacy and security requirements per the security and privacy policies of the HMIS;
- Maintain a CHO User roster, and submit a Helpdesk ticket when changes need to be made;
- Assist Users with problems and serve as an initial Helpdesk resource for Users at the CHO;
- Monitor data quality at least once a month;
- Work with the Associate Director of HMIS as necessary on data quality issues;
- Ensure that all critical and necessary HMIS information is disseminated to all Provides and Users (e.g. changes in data collection or data entry standards, or security updates);
- Prepare for HMIS audits;
- Complete annual Privacy training; and
- Serve as the HMIS Security Officer for the CHO.

CCHMIS End User

CCHMIS End Users are persons who access the HMIS with User accounts to perform job duties.

A CCHMIS End User must:

- Enter into the CCHMIS User Agreement and abide by all its requirements, including:
    1. HMIS Data collection requirements;
    2. HMIS Data entry requirements;
    3. HMIS use requirements; and
    4. Maintenance of client confidentiality.
- Maintain compliance with all required trainings and documentation.

CCHMIS Advisory Committee

A part of the CCHMIS governance structure, the CCHMIS Advisory Committee will provide ongoing supervision to, and guide the actions of, the HMIS Lead.

The CCHMIS Advisory Committee must:

- » Convene regularly to evaluate the HMIS and ensure it meets HUD requirements;
- » Report to communities on policies regarding: consumer privacy and confidentiality, reporting schedules, information sharing, software choices, and monitoring; and
- » Dictate the activation and deactivation of the CCHMIS Implementation Committee, as necessary.

CCHMIS Implementation Committee

A part of the CCHMIS governance structure , the CCHMIS Implementation Committee is a non-essential, temporary entity that will, on behalf of a Continuum, facilitate the implementation of the CCHMIS in a new community.

The Implementation Committee must:

- » Be activated and deactivated at the discretion of the CCHMIS Advisory Committee;
- » Convene regularly during active periods to support the HMIS Lead with research, evaluation, and negotiation of a contract with the HMIS vendor;
- » Assist in obtaining community support and coordinating the implementation of HMIS across the Continuum; and
- » Establish initial community goals for the HMIS.

HMIS Participation

The United States Department of Housing and Urban Development (HUD) requires all CoC and ESG funded grantees and sub-grantees to participate in their local Homeless Management Information System (HMIS). This policy is consistent with the Congressional Direction for communities to provide data to HUD on the extent and nature of homelessness and the effectiveness of its service delivery system in preventing and ending homelessness. The CCHMIS and its operating policies and procedures are structured to comply with the most recently released HUD Data and Technical Standards for HMIS. Recognizing that the Health Insurance Portability and Accountability Act (HIPAA) along with other Federal, State and local laws may further regulate agencies.

The Continuum of Care, in conjunction with the HMIS Lead, will work with all homeless service provider organizations within the geographic coverage area of the CoC to increase participation in HMIS to the benefit of the CoC. CoC-funded programs will be required to work with the HMIS Lead to participate in the HMIS, and non-CoC-funded programs required to participate in the HMIS may do so under individual HMIS service contracts with the HMIS Lead or the HMIS Vendor. Organizations with programs serving victims of abuse, neglect or domestic violence (victim service providers) will not be allowed to participate in the HMIS but will be required to provide the Continuum with data from a comparable database to meet federal reporting requirements.

Participation in the HMIS by organizations that do not receive HUD or federal partner funding is voluntary. However, the Continuum is strongly recommended to encourage participation by all homeless service provider organizations to achieve an accurate picture of homelessness within the CoC, as well as to aid the CoC in the grant competition (such as achieving service coverage and bed coverage rates, as per Federal Register Vol. 76, No. 237 § 580.37 Data quality standards and management).

Minimum Participation Requirements

- Collect all universal data elements, as defined by HUD, for all programs operated by the agency that primarily serve persons who are homeless, formerly homeless, or at risk of becoming homeless,
- For all programs, enter federally required client-level data into the HMIS.
- For all programs funded by the Department of Health and Human Services, or HUD, enter federally required client level data.
- Complete data entry within specific time frames, depending on the type or program.
- Comply with all HUD regulations for HMIS participation.

The CCHMIS uses all submitted data for analytic and administrative purposes, including the preparation of CCHMIS reports to funders and the Continuum's participation in the Longitudinal Systems Analysis and System Performance Measures reports submitted to HUD.

CHO Participation Requirements

- Authorized agency users directly enter client-level data into the HMIS database. Users have rights to access data for clients served by their agency and use HMIS functionality based on their user level privileges. The agency's data is stored in the HMIS central database server, which is protected by several levels of security to prevent access from unauthorized users.
- Each agency shall designate one Agency Administrator who is the agency's point person/specialist regarding HMIS. The Agency Administrator is responsible for:
    1. Providing agency specific information to the HMIS lead agency.
    2. Organizing its agency's users by requesting user access.
    3. Making sure proper training has taken place for the users and that all HMIS policies are being followed by all users from that agency; AND checking that all agency data is accurate.
    4. Notifying the HMIS lead agency of any staff turnover within 24 hours of an employee with HMIS access ending employment with the participating agency.

Privacy and Security Policies and Procedures

Privacy Requirements

Policy: All CHOs must comply with the baseline privacy requirements described here with respect to: data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability. A CHO may adopt additional substantive and procedural privacy protections that exceed the baseline requirements for each of these areas in its privacy notice. A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PII. When PII is shared between organizations, responsibilities for privacy and security may reasonably be allocated between the organizations (Section 4.2, 2004 HMIS Data and Technical Standards).

Procedure: All CHO policies regarding privacy requirements must at a minimum include the criteria following in this document. Additional requirements may be added at the discretion of each CHO.

Limits on Data Collection

Policy: A CHO may collect PII only when appropriate to the purposes for which the information is obtained or when required by law. A CHO must collect PII by lawful and fair means and, where appropriate, with the knowledge or consent of the individual (Section 4.2.1, 2004 HMIS Data and Technical Standards).

Procedure: A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting any and all information. Data allowable includes all HUD mandated data as well as any other data deemed necessary and approved by the CHO which complies with federal regulations and the policies and procedures of this document.

Additional Privacy Protections

Client Confidentiality

Policy: The CCHMIS Lead agency and CHOs will ensure the confidentiality of all client data. No identifiable client data will be entered into the CCHMIS without client consent, and no identifiable client data will be shared outside of the limits of that consent.

Procedure: Access to client data will be tightly controlled using security technology and restrictive access policies. Only individuals authorized to view or edit individual client data will have access to that data.

Informed Consent

Policy: CHOs will collect and retain signed client consent forms before any client PII will be entered into the CCHMIS. CHO staff will thoroughly explain the client consent to each client.

Procedure: Client consent forms must be completed with each individual or household accessing services before any information is entered into the CCHMIS. Consent forms should be stored in a secure place.

Policy: CHOs will collect and document verbal consent before any client PII is entered into the CCHMIS when clients call a Coordinated Entry Access Point with a housing crisis.

Procedure: Verbal consent to data collection and sharing must be documented by the person receiving the call from the client in housing crisis. If a client presents to an agency for Diversion or Referral, written consent should be sought and obtained before any additional data is collected and entered into the CCHMIS. Both documentation of verbal consent and subsequent signed consent forms should be stored in a secure place.

User Privacy Measures

Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

- Restricting collection of personal data, other than required HMIS data elements; • Collecting PII only with the express knowledge or consent of the individual (unless required by law); and
- Obtaining oral or written consent from the individual for the collection of personal information from the individual or from a third party (Section 4.2.1, 2004 HMIS Data and Technical Standards).

Procedure: All additional privacy measures must comply with federal regulations and the policies and procedures of this document.

Policy: CCHMIS End Users will be responsible for maintaining updated and accessible privacy notices and other procedures.

Procedure: All user policies must be available to staff members and clients. Changes to privacy notices should be given in advance to all clients and employees using a designated procedure developed by the CHO.

Required Data Collection

Policy: CHOs will collect all required sets of data variables for each client as determined by HUD HMIS Data and Technical Standards (see Appendix B for Required Data Elements).

Procedure: Appendix A will contain a listing of data elements to be collected for each client contact in accordance with federal regulations. These data elements may change as HUD HMIS Data and Technical Standards are revised and updated. For consistency in data collection and more accurate reporting, all participating programs may be held to the most stringent or numerous program-specific data collection requirements. The decision to add a data element to an assessment will be made by the CoC's with input from the HMIS Advisory Committee.

Appropriate Data Collection

Policy: PII collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PII should be accurate, complete and timely. CCHMIS End Users will only collect client data relevant to the delivery of services to people experiencing a housing crisis in their CoC (Section 4.2.2, 2004 HMIS Data and Technical Standards).

Procedure: CCHMIS End Users will refer to policies outlined in the Data Quality Plan for timelines, accuracy and completeness. Users will ask the CCHMIS lead agency for any necessary clarification of appropriate data collection.

Privacy Notice - Identifying Purpose and Use Limitation

Policy: A CHO must the CCHMIS privacy notice, located in the CCHMIS Informed Consent form the purposes for which it collects PII that describes all uses and disclosures. A CHO may use or disclose PII only if the use or disclosure is allowed by this standard and is described in the privacy notice (Section 4.2.3, 2004 HMIS Data and Technical Standards).

Procedure: A CHO may infer its ability to consented use and disclosure of any item specified in the notice. Except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards, all uses and disclosures are permissive and not mandatory. Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law. A CHO must take immediate actions to notify the CCHMIS lead agency about all legal disclosures.

Additional Uses

Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

- Seeking either oral or written consent for some or all processing when individual consent for a use, disclosure or other form of processing is appropriate;
- Agreeing to additional restrictions on use or disclosure of an individual's PII at the request of the individual if the request is reasonable. The CHO is bound by the agreement, except if inconsistent with legal requirements;
- Limiting uses and disclosures to those specified in its privacy notice and to other uses and disclosures that are necessary for those specified;
- Committing that PII may not be disclosed directly or indirectly to any government agency (including a contractor or grantee of an agency) for inclusion in any national homeless database that contains personal protected information unless required by statute;

- » Committing to maintain an audit trail containing the date, purpose and recipient of some or all disclosures of PII;
- » Committing to make audit trails of disclosures available to the homeless individual; and
- » Limiting disclosures of PII to the minimum necessary to accomplish the purpose of the disclosure (Section 4.2.3, 2004 HMIS Data and Technical Standards).

Procedure: Additional privacy protections beyond the baseline requirements are permissible, as exemplified in this policy. Protections should, however, be documented in the privacy notice at all times and approved by the CCHMIS lead agency if potentially beyond reasonable scope of authority.

Anonymous Clients

Rationale: Anonymous clients in HMIS negatively affect data quality for the Longitudinal System Analysis (LSA) and other HUD reports. HUD does allow for anonymous clients, but they also count that data as missing, and HUD funding is increasingly being tied to data quality. There is certainly a need to accommodate clients who need services, but who do not feel comfortable sharing their personally identifying information in HMIS. Having a clear understanding of the CCHMIS Privacy Policies is a necessity when explaining to clients what purpose their data fills and how it is protected. Based on previous years' data, CCHMIS providers have an average of less than 1% of clients not fleeing domestic violence being entered as anonymous.

Policy: The CHO's current year (October to September) percentage of anonymous clients not currently fleeing domestic violence shall not exceed 2% of its total clients served during the same period.

Procedure: Refer to the Data Quality Plan for information on how to find the percentage of anonymous clients not currently fleeing domestic violence for a given CHO.
(see Appendix A for Anonymization procedure)

Ethical Data

Policy: Data contained in the CCHMIS will only be used to support the delivery of homeless and housing services in each CoC. Each HMIS End User will affirm the principles of ethical data use and client confidentiality contained in this document.

Procedure: All HMIS End Users will sign an HMIS End User Agreement before being given access to the CCHMIS. Any individual or CHO misusing, or attempting to misuse HMIS data will be denied access to the database, and their relationship with the CCHMIS will be terminated.

Termination

Policy: All HMIS End Users and CHOs are subject to the privacy and confidentiality terms outlined in this document as well as the federal regulations in the HUD Data and Technical Standards. At any point if a breach of rules and/or policies occurs the user may be penalized by loss of access and/or membership in the CCHMIS.

Procedure: The CHO or HMIS End User shall inform the HMIS lead agency in a timely manner of any breach of the privacy and security policies outlined in this document or the HUD Data and Technical Standards. The HMIS lead agency will investigate the issue and determine a proper course of action for correction. If a permanent resolution is unforeseen or the HMIS lead agency deems it necessary, a CHO and/or user termination may occur:

- » The Partner Agency will be notified in writing of the intention to terminate their participation in the CCHMIS.

- The HMIS lead agency will revoke access of the HMIS End User or CHO staff to CCHMIS.
- The HMIS lead agency will keep all termination records on file.

Voluntary Termination

Policy: Should the CHO or HMIS End User decide not to comply with the rules and policies of this document and regulations in the HUD Data and Technical Standards for any reason, they may voluntarily terminate their user agreement with the CCHMIS.

Procedure: The CHO must use the following measures to terminate participation in the CCHMIS:

- The CHO or HMIS End User shall inform the HMIS lead agency in writing of their intention to terminate their agreement to participate in the CCHMIS.
- The HMIS lead agency will inform partners and any other relevant parties of the change.
- The HMIS lead agency will revoke access of the CHO and/or HMIS End User in the CCHMIS.
- The HMIS lead agency will keep all termination records on file.

Openness and Disclosures

Policy: A CHO must publish a privacy notice describing its policies and practices for the processing of PII and must provide a copy of its privacy notice to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page. A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. (Section 4.2.4, 2004 HMIS Data and Technical Standards).

Procedure: All amendments to the privacy notice must be consistent with the requirements of these privacy standards. A CHO must maintain permanent documentation of all privacy notice amendments. Copies of the current privacy notice must be available to all clients, including a sign stating the availability of its privacy notice to any individual who requests a copy. In addition, CHOs who receive federal financial assistance shall provide required information in languages other than English that are common in the community, if speaker of these languages are found in significant numbers and come into frequent contact with the program. *CHOs are also reminded that they are obligated to provide reasonable accommodations for persons with disabilities throughout the data collection process.

Note: This obligation does not apply to CHOs who do not receive federal financial assistance and who are also exempt from the requirements of Title III of the Americans with Disabilities Act because they qualify as “religious entities” under that Act.

Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

- Giving a copy of its privacy notice to each client on or about the time of first data collection.
- Adopting a policy for changing its privacy notice that includes advance notice of the change, consideration of public comments, and prospective application of changes (Section 4.2.4, 2004 HMIS Data and Technical Standards).

Procedure: All additional privacy protections must remain consistent with current HUD requirements and be present on the privacy notice.

Access and Correction

Policy: A CHO must consider any request by an individual for correction of inaccurate or incomplete PII pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information. A CHO

can reject repeated or harassing requests for access or correction (Section 4.2.5, 2004 HMIS Data and Technical Standards).

Procedure: In its privacy notice, a CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PII:

- Information compiled in reasonable anticipation of litigation or comparable proceedings;
- Information about another individual (other than a health care or homeless provider);
- Information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or
- Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual. A CHO must document requests for changes to an individual's PII.

A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial.

Below are the different parties' access levels to data and sharing capabilities. Any additional questions or concerns should be discussed with the HMIS lead agency

Covered Homeless Organization

Policy: CHOs will have access to retrieve any individual and aggregate data entered into the CCHMIS. When generating reports, users will be able to generate data from any records associated with their programs.

Procedure: The CCHMIS is a system with limited shared visibility between HUD, Locally Funded, RHY, STEHP, SSVF, and PATH providers. All client acknowledgement of data collection and consent to share data forms used by CHOs must indicate that the data entered into the CCHMIS is viewable by all users of the system.

HMIS Lead Agency

Policy: The HMIS lead agency will have access to retrieve all data in the CCHMIS. The System Administrator will not access individual client data for purposes other than maintenance and checking for data integrity. Any client-level data submitted to other parties for data analysis will be de-identified and encrypted.

Procedure: System Administrators will only publish or submit to funders aggregate data from the HMIS. If client-level data is submitted to a third party for research purposes, it will be deidentified and encrypted.

Client

Policy: Any client will have access on demand to view, or keep a printed copy of, their own records contained in the CCHMIS. All requests for client information will follow agency policy guidelines for release of information. The client will also have access to a logged audit trail of changes to those records. No client shall have access to another client's records in the CCHMIS. PII of minors is not entered into the CCHMIS without the consent of a parent. In cases where a parent provides consent to share the PII of a minor, but the minor disagrees with that consent, the wishes of the minor to keep their data private will be honored. Upon turning 18, an individual served by a CHO as a minor may choose to begin sharing previously unshared data or to relinquish consent to further sharing of data collected on them in the past. Should the parent of an individual who was served by a CHO as a minor request a copy of that data, the CHO will obtain consent from the individual before releasing any historical data to their parent.

Procedure: A client will provide a signed written request to a case manager to see the client's own record. The case manager, or any available staff person with CCHMIS access, will verify the client's identity and print all requested information. The case manager can also request a logged audit trail of the client's record from the HMIS lead agency. The HMIS lead agency will print this audit trail and forward it to the CHO for distribution to the client.

Public

Policy: The HMIS lead agency will address all requests for data from entities other than CHOs or clients. No individual client data will be provided to any group or individual that is neither the CHO, which entered the data, nor the client without proper authorization or consent.

Procedure: All requests for data from anyone other than a CHO or client will be directed to the HMIS lead agency. As part of the HMIS lead agency's regular functions, periodic public reports about homelessness and housing issues in each will be issued. No PII data will be released in any of these reports.

Inter-Agency Data Sharing

Policy: All client data entered into the CCHMIS is locked and only limited record information is viewable by all users with client consent.

Procedure: All client acknowledgements of data collection and consent to share data forms used by CHOs must indicate the client's preferred level of sharing.

Access to CCHMIS Database

Policy: No one will have direct access to the CCHMIS database unless explicitly given permission by CoC.

Procedure: In contract with CoC, Foothold Technology will monitor access of the database server and employ security methods to prevent unauthorized database access.

On-Site Review

Policy: The HMIS lead agency will perform annual on-site reviews at each CHO of data processes related to the CCHMIS.

Procedure: This review will be done as part of the annual Continuum of Care monitoring process.

Accountability

Policy: A CHO must adhere to confidentiality, privacy and security standards. A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices.

Procedure: Each CHO must develop and maintain a written copy of procedures for accepting and considering questions or complaints. This must be accessible to all staff members and updated as needed to comply with all HUD regulations. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice (Section 4.2.6, 2004 HMIS Data and Technical Standards).

Additional Protections

Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements. Additional corrections include but are not limited to:

- » Establishing a method, such as an internal audit, for regularly reviewing compliance with its privacy policy;
- » Establishing an internal or external appeal process for hearing an appeal of a privacy complaint or an appeal of a denial of access or correction rights; and/or
- » Designating a chief privacy officer to supervise implementation of the CHO's privacy standards.

Procedure: Any additional privacy protections should comply with all federal HUD HMIS Data and Technical Standards and policies in this document. Additional protections must be written out in each CHO's policies and procedures documents.

Client Grievance

Policy: Clients will contact the CHO with which they have a grievance for resolution of HMIS problems. CHOs will report all HMIS-related client grievances to the HMIS lead agency.

Procedure: Clients will bring HMIS complaints directly to the CHO with which they have a grievance. CHOs will provide a copy of the CCHMIS Policies and Procedures Manual upon request, and respond to client issues. CHOs will send written notice to the HMIS lead agency of any HMIS related client grievance. The HMIS lead agency will record all grievances and will report these complaints to the COC.

Policy: If the client is not satisfied with the results of the grievance with the CHO, the client may contact the HMIS lead agency for further assistance.

Procedure: Clients bringing HMIS complaints to the HMIS lead agency will be provided a copy of the CCHMIS Policies and Procedures Manual upon request. The HMIS lead agency will send written notice to the CHO of HMIS-related client grievance. The HMIS lead will record all grievances and will report these complaints to the CoC.

User Grievance

Policy: Users will contact HMIS lead agency with any grievance regarding HMIS. The HMIS lead agency will report all HMIS related user grievances to the CoC.

Procedure: Users will bring HMIS complaints directly to the HMIS lead agency. The HMIS lead agency will provide a copy of the CCHMIS Policies and Procedures Manual upon request, and respond to any user issues.

Policy: If the user is not satisfied with the results of the grievance with the HMIS lead agency, the user may contact their CoC for further assistance.

Procedure: Users bringing HMIS complaints to the CoC will be provided with a copy of the CCHMIS Policies and Procedures Manual upon request. The CoC will record all grievances and will make a final recommendation about how to respond to the grievance.

Security Standards

System Security

Policy: A CHO must apply system security provisions to all the systems where personally identifying information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mainframes and servers (Section 4.3.1, 2004 HMIS Data and Technical Standards).

Procedure: Each CHO must apply and maintain security provisions in the form of virus protection, firewalls, and other provisions listed below in this section to ensure the confidentiality of its clients.

Additional Security Protections

Policy: A CHO may commit itself to additional security protections consistent with HMIS requirements by applying system security provisions to all electronic and hard copy information that is not collected specifically for the HMIS. A CHO may also seek an outside organization to perform an internal security audit and certify system security (Section 4.3.1, 2004 HMIS Data and Technical Standards).

Procedure: Additional security protections may be utilized as each CHO believes necessary, but must be compliant with HMIS requirements.

Hardware/Software Requirements

Policy: CHOs will provide their own computer and method of connecting to the Internet, and thus the CCHMIS.

Procedure: It is the responsibility of the CHO to provide a computer and connection to the Internet. If desired by the CHO, the HMIS lead agency will provide advice as to the type of computer and connection.

Data Access Location

Policy: Users will ensure the confidentiality of client data, following all security policies in this document and adhering to the standards of ethical data use, regardless of the location of the connecting computer. All users are prohibited from accessing the HMIS database from any location other than the designated and approved work site.

Procedure: All Policies and Procedures and security standards will be enforced regardless of the location of the connecting computer. All HMIS related data entry will be processed at a designated and approved work site. The HMIS Agency Administrator will provide any additional clarification.

User Access

Policy: Only authorized users will have access to the CCHMIS via a username and password. Users will keep their access information confidential.

Procedure: The HMIS lead agency will provide usernames and initial passwords to each user upon completion of training and signing of user agreements and receipt of this Security and Privacy Policies and Procedures document. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Usernames will be unique for each user and will not be exchanged with other users. The sharing of username and passwords will be considered a breach of policy resulting in access being revoked. Passwords will be reset every 90 days. Agencies will notify HMIS lead agency immediately of employee reassignment to non-HMIS job responsibilities or termination so the login can be inactivated. Users not accessing the CCHMIS within 30 days will have their login inactivated.

Virus Protection

Policy: A CHO must protect systems that access HMIS from viruses by using commercially available virus protection software. It may also commit itself to additional security measures beyond this standard if in line with HMIS regulations.

Procedure: A CHO must regularly update virus definitions from the virus software vendor. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is accessed.

Firewalls

Policy: A CHO must protect systems the access HMIS from malicious intrusion behind a secure firewall. It may also commit itself to additional security measures beyond this standard if in line with HMIS regulations.

Procedure: Each CHO must maintain its own up to date firewall, however, each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization.

User Licenses

Policy: User licenses are controlled by COHHIO regardless of program access.

Procedure: Licenses are assigned once training is completed successfully.

HMIS End User Agreements

Policy: Each End User will sign an HMIS End User Agreement before being granted access to the CCHMIS. End User agreements must be updated annually in order to retain access to the CCHMIS. This process will coincide with annual privacy training for each user.

Procedure: Each year, the HMIS lead agency will instruct users on the process for completing the annual privacy training and obtaining and submitting an updated HMIS End User Agreement. These instructions will be sent to HMIS End Users via the CCHMIS End User Listserv as well as an announcement in the CCHMIS database. Upon receipt of the signed agreement by the HMIS lead agency, the user account will be updated to reflect that all requirements have been met. End Users who fail to send the updated agreement by the date specified in the instructions will lose access to HMIS until their agreement is received.

HMIS Agency and Agency Administrator Agreements

Policy: Each agency participating in the CCHMIS will sign an HMIS Agency Agreement and Agency HMIS Administrator Agreement before any data may be entered for its clients. This agreement will be updated annually.

Procedure: Each year, HMIS lead agency will instruct agencies on the process for completing and submitting an updated HMIS Agency Agreement and Agency HMIS Administrator Agreement. These instructions will be sent to CHO's via a Sign Now Document from the Grants and Contracts Department. Upon receipt of the agreements by the HMIS Lead Agency, the agency records will be updated to reflect that

all requirements have been met. Any agency that fails to send the updated Agency agreements by the date specified in the instructions will lose access to HMIS at the user level until the agreement is received.

Training

Policy: All users must be trained by the HMIS Lead Agency and sign an End User Agreement prior to receiving a login to the HMIS. Also, all users must complete an Annual Privacy Training and renew any agreements in order to maintain access to the HMIS.

Procedure: CHO Agency Administrators or Executive Directors can sign up new or current users for HMIS training via the CARES of NY, Inc. website's HMIS training page. CCHMIS staff will provide training to all new users. Agency Administrators will be given additional training relevant to their position. CCHMIS staff will provide periodic training updates for all users. The HMIS lead agency will be responsible for ensuring that users are instructed in both policies and security.

Procedure: All users are required to complete an annual security and privacy training. Failure to complete this training may result in revocation of access to the CCHMIS.

Data Retrieval

Policy: HMIS End Users will maintain the security of any client PII data extracted from the database and stored locally, including all data used in custom reporting. HMIS End Users will not electronically transmit any PII client data across a public network.

Procedure: PII data extracted from the database and stored locally will be stored in a secure location and will not be transmitted outside of the private local area network. Security questions will be addressed to the HMIS lead agency.

Hard Copy Security

Policy: A CHO must secure any paper or other hard copy containing PII that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms. CHO may commit itself to additional security protections consistent with HMIS requirements by applying hard copy security provisions to paper and hard copy information that is not collected specifically for the HMIS (Section 4.3.2, 2004 HMIS Data and Technical Standards).

Procedure: A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PII when the hard copy is in a public area. When CHO staff is not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location.

Physical Access

Policy: A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff is not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. A CHO may commit itself to additional security protections consistent with HMIS requirements.

Procedure: A CHO must take steps to secure each computer by automatically turning on a password protected screen saver when the workstation is temporarily not in use. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system.

CHO Technical Support Requirements

Policy: CHOs will provide their own technical support for all hardware and software used to connect to the CCHMIS.

Procedure: CHOs will provide technical support for the hardware, software and Internet connections necessary to connect to the CCHMIS according to their own organizational needs.

Data Quality

Data Entry

Policy: HMIS End Users will be responsible for the accuracy of their data entry.

Procedure: The CHO must maintain standards for periodically checking data for completeness, accuracy and timeliness. The HMIS lead agency maintains Data Quality Standards to help all CHOs manage the monitoring of their data quality. The HMIS lead agency runs data quality reports monthly. The CCHMIS team contacts the End Users for the projects with the highest percentage of errors. If the End Users do not respond, CCHMIS staff will reach out to the Agency HMIS Administrator and/or Executive Director of the agency. If an agency does not adequately respond to the request for improvement, the issue will be raised with the CoC's Data Committee at the next scheduled meeting and an action plan determined. If the agency still does not adequately respond to the request for improvement, the CoC's Collaborative Applicant may contact the appropriate funding agency regarding the issue and continued access to the CCHMIS may be jeopardized.

Data Quality Plan

Policy: The Data Quality Standards, designed by HMIS lead agency in collaboration with HMIS Advisory Committee, is the official document pertaining to all data quality measures including but not limited to accuracy, completeness and timeliness. This should be referenced for all data quality standards. Any questions about materials in this document or items that are unclear should be addressed with the HMIS lead agency.

Procedure: The Data Quality Standards should be referenced and followed for all data quality procedures. Each CHO must retain copies of this document and have available for all relevant staff members. If questions are left unaddressed, they should be brought to the attention of HMIS lead agency in a timely manner.

New Provider Data

Policy: All new programs, projects or providers are to be created in the HMIS by HMIS lead agency.

Procedure: New programs, projects or providers are to send requested additions to the CCHMIS lead agency. Once received, the HMIS lead agency will enter the appropriate data into the CCHMIS.

Policy: All provider data including but not limited to name, project type, bed counts, address, and contact information in HMIS must be kept up to date.

Procedure: Any requests to change a provider's data are to be sent HMIS lead agency. Once received, the HMIS lead agency will enter the appropriate data into the CCHMIS.

HMIS Fees

Fees for use of the CCHMIS are determined by the CARES of NY, Inc. Executive Director in coordination with the Grants and Contracts Department.

Excess Active User Fee

Policy: A CHO will maintain an active User roster that does not exceed fifteen (15) Users at any given point in time. Any fees the HMIS Lead incurs from the HMIS vendor due to a CHO with excess active Users will be billed to that CHO. The HMIS Lead reserves the right to bill the CHO for administrative fees due to additional HMIS Lead staff time necessary to train and manage the HelpDesk for the increased number of Users.

Procedure: Fees will be billed to a CHO at the HMIS software vendor rate

TOTAL USERS	TOTAL CHO COST (PER MONTH)
16-30	$500
31-45	$1,000
46-60	$1,500
61-75	$2,000
71+	(Separate contract with vendor required)

***Please note**: the HMIS Lead does not receive additional income from fees for excess active Users. These fees are determined by the HMIS Vendor and are passed on by the HMIS Lead with no additional charges added by the HMIS Lead.*

Exemptions

This policy does not apply to Vendor CHOs.

Base Technical Assistance Rate

Current HMIS Lead base hourly rate for technical assistance: $100/hour

This rate is subject to change depending on the demands of a project.

Appendices

A. Anonymization Procedure

1. A client that does not consent to HMIS PII data entry **must still** have their information collected for services as per CHO policies and procedures on **paper** forms. Best practice would be to record the unique Client ID that AWARDS assigns to the HMIS record on the paper intake form and/or folder so that agency staff can trace it back appropriately for reporting and services purposes.
2. For Coordinated Entry (CE) purposes, this anonymized record may stand in as a placeholder in the by-name list. Each CE lead must establish how the rest of the information will be communicated and whether or not the vulnerability index (minus Protected Personal Information) should be entered into the HMIS, or if the score will be entered manually by the list manager for case conferencing purposes.
3. The User entering the client's record into the HMIS must not enter personal identifiers for First Name, Last Name, Social Security Number, or Date of Birth, and instead must fill out the required UDE data elements within the record as follows (and summarized within *Table 11*):
    a. All possible data elements must be set to "Client prefers not to answer" within the HMIS, including:
        i. **NAME DATA QUALITY**;
        ii. **SOCIAL SECURITY NUMBER DATA QUALITY**;
        iii. **BIRTHDATE DATA QUALITY**;
    b. **FIRST NAME**: Enter "Anon" into the field.
    c. **LAST NAME**: Enter a client identifier into the field that allows the CHO to recognize the anonymous record in the system, as per the following format: *
        i. The agency name or acronym and the 6 digit date of admission and USER initials
        ii. Kelli Clark enters John Doe into CARES Housing on 1/1/20: CARES010120KC
        iii. In the unlikely occurrence that there is more than one anonymous entry into an agency by the same user in a single day, add alphabetical identifiers; CARES010120KCa (b,c,d, etc.)
    d. **SOCIAL SECURITY NUMBER**: Enter the number 9 for all 9 digits into the field.
    e. **BIRTHDATE**: Enter January 1st of the client's birth year into the field.
4. Additional Household Members:
    a. **FIRST NAME**: Enter the relationship into the field such as "Child1", "Child2", "Child3", "Partner", "Parent", "Relative".
    b. **LAST NAME**: Use the same identifier for all household members (please see 3c above)
    c. **SOCIAL SECURITY NUMBER**: Enter the number 9 for all 9 digits into the field.
    d. **BIRTHDATE**: Enter January 1st of the CURRENT year into the field for minors and January 1st of the client's birth year for other adults into the field.

Table 1. Summary of data entry for a record without PII/anonymous record.

HMIS DATA FIELD	VALUE FOR USER TO ENTER	EXAMPLE
FIRST NAME	Enter "Anon"	Anon
LAST NAME	The client identifier for the client	CARES010120KC
NAME DATA QUALITY	Select "Client prefers not to answer"	
SOCIAL SECURITY NUMBER	Enter the number 9 for all 9 digits.	999-99-9999
SOCIAL SECURITY NUMBER DATA QUALITY	Select "Client prefers not to answer"	
BIRTHDATE	Enter January 1st of the year of the client's birth	01/01/1980
BIRTHDATE DATA QUALITY	Select "Client prefers not to answer"	

B. Required Data Elements

Universal Data Elements (UDE's)

The UDEs are baseline data collection elements required for all projects entering data into the HMIS. HMIS categories A, B, and C are required to input the following UDEs:

Name	Social Security Number	Date of Birth
Race & Ethnicity	Gender Identity	Veteran Status
Disabling Condition	Project Start Date	Project Exit Date
Exit Destination	Prior Living Situation	Relationship to Head of Household
Enrollment CoC	Housing Move- In Date	

Common Program Specific Data Elements (CPSE's)

CPSE's differ from the Universal Data Elements (UDEs) in that no one project must collect every single element in this section. Required data elements are dictated by the reporting requirements set forth by each Federal partner for the projects they fund. A Partner may require all or a selection of the fields or response categories.

Income and Sources	Non-Cash Benefits	Health Insurance
Physical Disability	Developmental Disability	Chronic Health Condition
HIV/AIDS	Mental Health Disorder	Substance Use Disorder
Domestic Violence	Current Living Situation	Date of Engagement
Coordinated Entry Assessment	Coordinated Entry Event	

Additional Program Specific Data Elements are outlined in the CCHMIS Data Quality Plan

C. CHO Verbal Explanation of the CCHMIS

Please verbally describe the HMIS and the terms of consent to clients at intake.

1. Explanation of HMIS:
    a. Computer based information system that homeless services agencies across the state use to capture information about the persons they serve.
    b. CCHMIS – the local system used at this agency.
2. Why the agency uses it:
    a. Federal mandate that all HUD funded homeless providers must enter data into an electronic system and capture universal data elements.
    b. Important to collect the data because the data is:
        i. Critical to gain an accurate count of the homeless population.
        ii. Analyzed for service use patterns to improve the success of interventions.
        iii. Used to better understand clients' needs.
        iv. Used to more accurately inform public policy and the organizations that provide the funds to run this and other homeless service programs.
            1. Critical to obtain funds.
        v. Used to plan to have appropriate resources for the people being served.
3. Security & Privacy measures:
    a. Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records.

b. All staff must sign agreements to maintain client confidentiality, with penalties for violation.
c. No information will be shared to another agency without written consent.
d. Client has the right to not answer any question they are not comfortable with, unless entry into a program requires it.
e. Client information is transferred via secure connection, in an encrypted format, to the CCHMIS.
f. Client has the right to know who has added to, deleted, or edited their CCHMIS record and may request this information.

4. Client information in HMIS:
   a. Client is not required to have their personally identifying information within the HMIS but encouraged to help the program meet requirements to continue to receive its funding.
5. Data sharing:
   a. Describe: Data sharing shares a client's program history and personal information from a project to others within the CCHMIS
      i. Case manager and client can use information to assist clients in obtaining resources that will help them find and keep permanent housing.
      ii. Other agencies can see your information to streamline and future intakes, to provide more informed care decisions.
   b. Inform client of the services offered on site and those offered via referral through an assessment process.

Inform client that this is their choice

D. Relevant Terminology

» **Continuum of Care (Continuum)** means the group composed of representatives from organizations including nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve veterans, and homeless and formerly homeless persons organized to carry out the responsibilities of a Continuum of Care established under 24 CFR part 578.

1. **"CoC"** is used when *not* referring to the group of people responsible for the operation of the CoC; i.e., CoC is used when referring to the funding source of HUD: Continuum of Care "**CoC-funded**" or when referring to the geographic coverage area of the CoC.
2. The term Continuum of Care or CoC is used throughout the remainder of this notice to refer to the parties that are typically responsible for developing and managing the local HMIS[2]
3. · Continuum project refers to a distinct unit of an organization, which may or may not be funded by HUD or the Federal Partners, whose primary purpose is to provide services and/or lodging for the homeless and is identified by the Continuum as part of its service system. For example, a project funded by the HUD's CoC Program may be referred to then as a "CoC Program-funded continuum project."
4. • CoC Program refers to the HUD funding source which provides housing and/or service grant dollars.

» **Comparable database** means a database that is not the Continuum's official HMIS, but an alternative system that victim service providers and legal services providers may use to collect client-level data over time and to generate unduplicated aggregate reports based on the data, and that complies with the requirements of this part. Information entered into a comparable database must not be entered directly into or provided to an HMIS.

[2] 2004 HMIS

- **Contributing HMIS Organization (or CHO)** means an organization (including its employees, volunteers, affiliates, contractors, and associates) that operates a project that contributes Protected Identifying Information (PII) on homeless clients to an HMIS.
- **End User** means an individual who uses or enters data in an HMIS or another administrative database from which data is periodically provided to an HMIS.
- **Homeless Management Information System (HMIS)** means the information system designated by Continuums of Care to comply with the requirements of this part and used to record, analyze, and transmit client and activity data in regard to the provision of shelter, housing, and services to individuals and families who are homeless or at risk of homelessness.
- **HMIS Lead** means an entity designated by the Continuum of Care in accordance with this part to operate the Continuum's HMIS on its behalf.
- **HMIS Vendor** means a contractor who provides materials or services for the operation of an HMIS. An HMIS vendor includes an HMIS software provider, web server host, data warehouse provider, as well as a provider of other information technology or support.
- **Protected identifying information (PII)** means information about a program participant that can be used to distinguish or trace a program participant's identity, either alone or when combined with other personal or identifying information, using methods reasonably likely to be used, which is linkable to the program participant.
- **Victim service provider** means a private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking. This term includes rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs.